

**WORKMAN, NYDEGGER & SEELEY**  
A PROFESSIONAL CORPORATION  
ATTORNEYS AT LAW  
1000 EAGLE GATE TOWER  
60 EAST SOUTH TEMPLE  
SALT LAKE CITY, UTAH 84111

## **BACKGROUND OF THE INVENTION**

### **1. Cross-Reference to Related Applications**

The present application claims the benefit of United States provisional application serial number 60/189,096, filed 14 March 2000, which provisional application is incorporated herein by reference.

### **2. The Field of the Invention**

The present invention relates to computer networks. Specifically, the present invention relates to methods and system for preventing socket flooding during denial of service attacks.

### **3. The Prior State of the Art**

Computer networks, and in particular the Internet, have transformed the way people communicate and do business. In these computer networks, computer systems may often communicate using a request/response protocol. For example, a requesting client computer system ("client") will transmit a request for a service to a responding server computer system ("server"). The responding server then uses data from within the request in order to fulfill the request.

For example, a client may compose a request for a Web page. In such a request, there would typically be request data such as the Uniform Resource Locator ("URL") identifying the Web page, the address of the client, and any other data that would be needed or helpful for the server to retrieve the Web page and transmit that Web page to the client. For each request, a typical server would allocate resources such as memory space,

1 processing time or pooled function calls for receiving the request data. Upon processing of  
2 the request data, the server would then free up these allocated resources.

3 While the vast majority of individuals use computer networks in a responsible  
4 manner, there are a few individuals who maliciously desire to harm others using computer  
5 networks. One particular harmful scheme is to impair the operation of another's server.  
6 This may be accomplished by, for example, repeatedly transmitting requests to the server  
7 without sending any request data.

8 Unaware of the malicious nature of the attack, the server will unknowingly attempt  
9 to accommodate each request by allocating memory, processing time and/or pooled  
10 function calls for each request. However, in the described harmful scheme, since no  
11 request data is sent, the server cannot finish processing the request until it has received data  
12 from the client. Until it has finished processing the request, the allocated resources are tied  
13 up and unavailable for subsequent requests. The server will eventually time out the  
14 connection and reclaim the resources after a certain time, but the timeout period is  
15 relatively long compared to the time it takes an attacker to flood the computer with  
16 requests. Eventually, during this timeout period, the server will deplete its ability to  
17 allocate resources resulting in denials of service for subsequent legitimate requests during  
18 the timeout period. This effectively shuts down operation of the server during the timeout  
19 period resulting in a loss of service for legitimate requests.

20 Therefore, what are desired are methods and systems for reducing the incidence of  
21 service denials due to an attack in which requests are repeatedly made to the server without  
22 transmitting any request data.

## SUMMARY OF THE INVENTION

The present invention relates to methods and systems for preventing or at least reducing the impact of denial of service attacks. Denial of service attacks occur when a client repeatedly sends connection requests to a server without sending corresponding request data. Without adequate protection, the server will allocate resources for each connection request. However, since no request data is sent, the server cannot finish processing the request and sits idle waiting for data from the client. The resources are hence not freed up for subsequent requests. Eventually, the resources are expended to a point where the server cannot respond to any other requests, legitimate or not. Thus, the server is effectively shut down by the denial of service attack.

In accordance with the present invention, an effective method of reducing the impact of denial of service attacks is presented. In one embodiment, the method is implemented in large part using Winsock modules. For each connection request received by the server from one or more clients, the server attempts to establish a connection to accommodate the corresponding request. In the Winsock implementation, the Winsock extension Winsock()AcceptEx() is used to try to establish a connection.

Next, the connection request is mapped to a corresponding listen socket. For each connection request that the server cannot currently handle, the connection request is placed in the backlog queue corresponding to the listen socket to which the connection request mapped. The backlog queues are monitored, for example, by calling a Winsock()select() module and passing in those listen sockets that correspond to the monitored backlog queues. The backlog queues are determined to be used, for example, if the Winsock()select() module returns.

1 If one or more of the backlog queues have entries, then the method determines  
2 which connection sockets have connections but no corresponding request data. This  
3 identification may be accomplished using, for example, the Winsock(getsockopt()  
4 module. These connection sockets are suspected to be serving a malicious connection  
5 request since there is a connection but no request data received which is indicative of a  
6 denial of service attack. Thus, these connection sockets are disconnected.

7 The present invention allows for the early detection of denial of service attacks by  
8 immediately taking action once the backlog queue has entries, rather than waiting until the  
9 server becomes dysfunctional. If a denial of service attack were to occur, highly suspect  
10 connection sockets corresponding to the denial of service attack would be disconnected  
11 thereby freeing up resources for legitimate requests. Even if the denial of service attack  
12 were to continue, the method would continue to disconnect the maliciously established  
13 connections thereby allowing more legitimate connection requests to be satisfied even  
14 during the denial of service attack. This improves the security of the server against denial  
15 of service attacks and diminishes the malicious motive for generating denial of service  
16 attacks in the first place.

17 There is some risk associated with closing a connection socket simply when it has a  
18 connection but no received data. For example, the connection socket may not have been  
19 created as a result of a malicious connection request. Instead, it may be that the connection  
20 request was legitimate in that the associated connection socket just happened to be in a  
21 stage where the connection was just made but the soon to arrive request data simply has  
22 not arrived yet. In this case, a legitimate connection request would be denied.

23 However, this case would typically be relatively rare. For example, the legitimate  
24 connection request would not be denied unless the backlog queue had entries in it which

Docket No. 13768.143

**BRIEF DESCRIPTION OF THE DRAWINGS**

In order that the manner in which the above-recited and other advantages and features of the invention are obtained, a more particular description of the invention briefly described above will be rendered by reference to specific embodiments thereof which are illustrated in the appended drawings. Understanding that these drawings depict only typical embodiments of the invention and are not therefore to be considered to be limiting of its scope, the invention will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

Figure 1 illustrates an exemplary system that provides a suitable operating environment for the present invention;

Figure 2 is schematically illustrates a client and server communicating using a standard request/response protocol;

Figure 3 illustrates a server-implemented process for responding to requests;

Figure 4 illustrates a series of listen sockets implements using a Winsock module as existing on a server; and

Figure 5 illustrates a server-implemented method of protecting against or at least reducing the impact of denial of service attacks.

## DETAILED DESCRIPTION OF THE INVENTION

The present invention extends to both methods and systems for preventing denial of services due to socket flooding caused by a denial of service attack. The embodiments of the present invention may comprise a special purpose or general purpose computer including various computer hardware, as discussed in greater detail below.

Embodiments within the scope of the present invention also include computer-readable media for carrying or having computer-executable instructions or data structures stored thereon. Such computer-readable media can be any available media which can be accessed by a general purpose or special purpose computer. By way of example, and not limitation, such computer-readable media can comprise RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to carry or store desired program code means in the form of computer-executable instructions or data structures and which can be accessed by a general purpose or special purpose computer. When information is transferred or provided over a network or another communications connection (either hardwired, wireless, or a combination of hardwired or wireless) to a computer, the computer properly views the connection as a computer-readable medium. Thus, any such a connection is properly termed a computer-readable medium. Combinations of the above should also be included within the scope of computer-readable media. Computer-executable instructions comprise, for example, instructions and data which cause a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions.

Figure 1 and the following discussion are intended to provide a brief, general description of a suitable computing environment in which the invention may be



1 implemented. Although not required, the invention will be described in the general context  
2 of computer-executable instructions, such as program modules, being executed by  
3 computers in network environments. Generally, program modules include routines,  
4 programs, objects, components, data structures, etc. that perform particular tasks or  
5 implement particular abstract data types. Computer-executable instructions, associated  
6 data structures, and program modules represent examples of the program code means for  
7 executing steps of the methods disclosed herein. The particular sequence of such  
8 executable instructions or associated data structures represent examples of corresponding  
9 acts for implementing the functions described in such steps.

10 Those skilled in the art will appreciate that the invention may be practiced in  
11 network computing environments with many types of computer system configurations,  
12 including personal computers, hand-held devices, multi-processor systems,  
13 microprocessor-based or programmable consumer electronics, network PCs,  
14 minicomputers, mainframe computers, and the like. The invention may also be practiced  
15 in distributed computing environments where tasks are performed by local and remote  
16 processing devices that are linked (either by hardwired links, wireless links, or by a  
17 combination of hardwired or wireless links) through a communications network. In a  
18 distributed computing environment, program modules may be located in both local and  
19 remote memory storage devices.

20 With reference to Figure 1, an exemplary system for implementing the invention  
21 includes a general purpose computing device in the form of a conventional computer 120,  
22 including a processing unit 121, a system memory 122, and a system bus 123 that couples  
23 various system components including the system memory 122 to the processing unit 121.  
24 The system bus 123 may be any of several types of bus structures including a memory bus

1 or memory controller, a peripheral bus, and a local bus using any of a variety of bus  
2 architectures. The system memory includes read only memory (ROM) 124 and random  
3 access memory (RAM) 125. A basic input/output system (BIOS) 126, containing the basic  
4 routines that help transfer information between elements within the computer 120, such as  
5 during start-up, may be stored in ROM 124.

6 The computer 120 may also include a magnetic hard disk drive 127 for reading  
7 from and writing to a magnetic hard disk 139, a magnetic disk drive 128 for reading from  
8 or writing to a removable magnetic disk 129, and an optical disk drive 130 for reading  
9 from or writing to removable optical disk 131 such as a CD-ROM or other optical media.  
10 The magnetic hard disk drive 127, magnetic disk drive 128, and optical disk drive 130 are  
11 connected to the system bus 123 by a hard disk drive interface 132, a magnetic disk drive-  
12 interface 133, and an optical drive interface 134, respectively. The drives and their  
13 associated computer-readable media provide nonvolatile storage of computer-executable  
14 instructions, data structures, program modules and other data for the computer 120.  
15 Although the exemplary environment described herein employs a magnetic hard disk 139,  
16 a removable magnetic disk 129 and a removable optical disk 131, other types of computer  
17 readable media for storing data can be used, including magnetic cassettes, flash memory  
18 cards, digital video disks, Bernoulli cartridges, RAMs, ROMs, and the like.

19 Program code means comprising one or more program modules may be stored on  
20 the hard disk 139, magnetic disk 129, optical disk 131, ROM 124 or RAM 125, including  
21 an operating system 135, one or more application programs 136, other program modules  
22 137, and program data 138. A user may enter commands and information into the  
23 computer 120 through keyboard 140, pointing device 142, or other input devices (not  
24 shown), such as a microphone, joy stick, game pad, satellite dish, scanner, or the like.

1 These and other input devices are often connected to the processing unit 121 through a  
2 serial port interface 146 coupled to system bus 123. Alternatively, the input devices may  
3 be connected by other interfaces, such as a parallel port, a game port or a universal serial  
4 bus (USB). A monitor 147 or another display device is also connected to system bus 123  
5 via an interface, such as video adapter 148. In addition to the monitor, personal computers  
6 typically include other peripheral output devices (not shown), such as speakers and  
7 printers.

8 The computer 120 may operate in a networked environment using logical  
9 connections to one or more remote computers, such as remote computers 149a and 149b.  
10 Remote computers 149a and 149b may each be another personal computer, a server, a  
11 router, a network PC, a peer device or other common network node, and typically include  
12 many or all of the elements described above relative to the computer 120, although only  
13 memory storage devices 150a and 150b and their associated application programs 136a and  
14 136b have been illustrated in Figure 1. The logical connections depicted in Figure 1  
15 include a local area network (LAN) 151 and a wide area network (WAN) 152 that are  
16 presented here by way of example and not limitation. Such networking environments are  
17 commonplace in office-wide or enterprise-wide computer networks, intranets and the  
18 Internet.

19 When used in a LAN networking environment, the computer 120 is connected to  
20 the local network 151 through a network interface or adapter 153. When used in a WAN  
21 networking environment, the computer 120 may include a modem 154, a wireless link, or  
22 other means for establishing communications over the wide area network 152, such as the  
23 Internet. The modem 154, which may be internal or external, is connected to the system  
24 bus 123 via the serial port interface 146. In a networked environment, program modules

1 depicted relative to the computer 120, or portions thereof, may be stored in the remote  
2 memory storage device. It will be appreciated that the network connections shown are  
3 exemplary and other means of establishing communications over wide area network 152  
4 may be used.

5 Figure 2 illustrates a requesting client computer system 210 (hereinafter, "a client")  
6 and a responding server computer system 220 (hereinafter, "a server") which communicate  
7 over a network 230. In a typical request/response communication protocol such as  
8 HyperText Transport Protocol ("HTTP"), the client 210 transmits a connection request 240  
9 to the server 220 over the network 230. The server 240 then provides a connection in  
10 response to the connection request and transmits a connection confirmation message 250  
11 back to the client 210. The client 210 then transmits request data 260 to the server 220.  
12 The request data 260 includes information helpful in identifying what the request is as well  
13 as information helpful in fulfilling the request. If appropriate for the request, the server  
14 220 then transmits a response 270 back to the client 210 over the network 230.

15 The server computer system 220 is a "server" computer system in that it provides a  
16 service in the form of a connection and a response to the client computer system 210. The  
17 server may also obtain the services of other computer systems over the network. In this  
18 context, the server 220 may also be a client computer system. The client computer system  
19 210 is a "client" computer system in that it is served by the server providing the connection  
20 and generating the response. The client computer system 210 may provide services to yet  
21 other computer systems. In this context, the client computer system may also be a server  
22 computer system. The client 210 and the server 220 may each be structure similar to the  
23 computer 120 or may contain a subset or superset of the elements described above for the  
24 computer 120.

1 Figure 3 illustrates a flowchart of a method 300 performed by the server 220 when  
2 responding to requests from the client 210. The method is initiated by the server 220  
3 monitoring the network 230 for connection requests destined for the server 220 (step 310).  
4 The method continues as the server 220 detects such connection requests (step 320). The  
5 remainder of the method 300 is performed for each detected connection request.

6 For each connection request, a connection is established using a means or step for  
7 establishing a connection request. Specifically, for each connection request, the  
8 connection request is mapped to a specific listen socket (step 330). If the server is  
9 implementing the WINDOWS ® operating system, the server may call a Winsock module  
10 to map the request to the listen socket. Figure 4 schematically illustrates a Winsock  
11 module 410 and associated listen sockets 420 and will be used in describing the remaining  
12 steps of Figure 3. As apparent to those of ordinary skill in the art, a listen socket allows  
13 the server to listen for the expected request data. The Winsock module may create one or  
14 more listen sockets 420A through 420H. Step 330 maps the request to one of these listen  
15 sockets 420.

16 If the server is able to accommodate the connection request ("Yes" in decision  
17 block 340), the server allocates resources (step 360) such as memory space, processing  
18 time or pooled function calls for receiving and processing the expected request data. The  
19 server computer system then receives the request data (step 370) and processes the request  
20 data (step 380). Once the server has completed processing the request, the server frees up  
21 the previously allocated resources and disconnects (step 390).

22 On the other hand, if the server 220 is unable to handle the connection request  
23 ("No" in decision block 340), then the connection request is placed in a backlog queue for  
24 future handling (step 350). As shown in Figure 4, each listen socket 420A through 420H

1 has a corresponding backlog queue 430A through 430H. If the server cannot handle the  
2 connection request, the connection request is passed into the queue corresponding to the  
3 listen socket that the connection request mapped to in step 330. Although each listen  
4 socket has a request queue in Figure 4, in an alternative embodiment, a more general  
5 backlog queue may be shared between one or more or all of the listen sockets. In this  
6 alternative, the server computer system may map the request to the listen socket after the  
7 connection request is drawn from the backlog queue during future processing.

8 The method 300 will now be explained in the context of a WINDOWS ® operating  
9 system using a Winsock module to establish connections. For each detected connection  
10 request, the Winsock module maps the connection request to a listen socket (step 330). To  
11 establish a connection to the listen socket, a module may be called that accepts connections  
12 and waits for request data before completing. For example, an extension of the Winsock  
13 module called Winsock()AcceptEx() is called and the corresponding listen socket is passed  
14 in along with the new connection socket that represents the connection to the listen socket.  
15 The Winsock()AcceptEx() is completed when request data is beginning to be received  
16 from the network in step 370.

17 Winsock may allocate a pool having a fixed number of Winsock()Accept() calls  
18 available for creating new connections. If the entire pool of Winsock()Accept() calls are  
19 already processing new connections, then the server is not currently able to satisfy  
20 subsequent connection requests ("No" in decision block 340). In this case, the connection  
21 request is placed in the backlog queue corresponding to listen socket (step 350).

22 In normal operation, it should preferably be very rare that the server 220 cannot  
23 currently handle a connection request. However, a denial of service attack may often result  
24 in the server being unable to currently handle connection requests. In this description and

1 in the claims, a “denial of server attack” is defined as the repetitious transmission of  
2 connection requests without a subsequent transmission of request data needed to process  
3 the requests. In such a denial of service attack, the method 300 of Figure 3 will proceed  
4 through step 360 in which resources are allocated. However, the server does not receive  
5 subsequent request data as in step 370. Therefore, the allocated resources are never freed  
6 up in step 390. Since connection requests are repeatedly made, the amount of allocated  
7 resources rises until the server can no longer allocate resources and thus must deny  
8 legitimate requests for service.

9 In the context of the Winsock module, the repeated connection requests will result  
10 in repeated calls of the Winsock()AcceptEx() module. However, none of the  
11 Winsock()AcceptEx() modules will complete since no request data is sent during a denial  
12 of service attack. Thus, the pool of Winsock()AcceptEx() modules will gradually deplete.  
13 Eventually, the server 220 will not be able to handle new connection requests, legitimate or  
14 not, and the connection requests will be placed in the backlog queue. Eventually, the  
15 backlog queue will also be filled up and thus new connection requests will not be saved  
16 and thus will never be handled.

17 Figure 5 illustrates a flowchart of a method 500 that prevents or at least reduces the  
18 impact of these denial of service attacks. As mentioned above, when the server 220 cannot  
19 currently handle a connection request, the connection request is place in a backlog queue.  
20 The method 500 monitors this backlog queue (step 510). Accordingly, embodiments  
21 within the scope of the present invention include a means and/or step for monitoring the  
22 backlog queue. Any method of monitoring the backlog queue will suffice so long as the  
23 method is capable of determining whether of not there are entries in the backlog queue. In  
24 the example shown in Figure 4, each listen socket has a corresponding backlog queue. The

1 method 500 may monitor these backlog queues by, for example, calling modules that scan  
2 the backlog queues to determine usage. On such module is a Winsock extension called  
3 Winsock()select(). A list of listen sockets is passed into the Winsock()select() function.  
4 The Winsock()select() module monitors the backlog queue of each of the listens sockets in  
5 the list of listen sockets passed into the Winsock()select() module.

6 Next, the method 500 determines if the backlog queue is being used (step 520).  
7 Any method for determining that the backlog queue is being used will suffice. In the  
8 above example where the Winsock()select() extension of Winsock is used to monitor the  
9 backlog queue, the determination is made by the very fact that the  
10 Winsock()select()extension module returns. The Winsock()select() extension module  
11 returns when one or more of the listen sockets have entries in their corresponding backlog  
12 queues.

13 Next, the method 500 resets one or more connection sockets upon notification that  
14 the backlog queue is being used (step 530). Accordingly, embodiments within the scope of  
15 the present invention include a means and/or step for resetting one or more connection  
16 sockets upon notification that the backlog queue is being used.

17 As part of the step for resetting one or more listen sockets, the method 500 includes  
18 a step of determining which connection sockets have established connections, but have not  
19 received any data (step 540). In the context of using Winsock, the server computer system  
20 220 enumerates all the connection sockets that have been created using a currently called  
21 Winsock()AcceptEx() function. For each of these currently called Winsock()AcceptEx()  
22 connection sockets, the extension Winsock()getsockopt() is used to determine whether or  
23 not a connection has been established. If a connection has been established, then the  
24 connection socket is suspected of being caused by a malicious connection request since a



1 connection has been made, yet no request data has been sent (otherwise, the  
2 Winsock()AcceptEx() module would not be currently called but would have been  
3 completed). Thus, this connection socket may be disconnected (step 550) since it is  
4 assumed that a connection socket having a connection but no request data is most likely the  
5 result of a denial of service attack.

6 There is some risk associated with closing a connection socket simply because it  
7 has a connection but no received request data. For example, the connection socket may not  
8 have been created as a result of a malicious connection request. Instead, it may be the  
9 connection request was legitimate in that the associated connection socket just happened to  
10 be in a stage where the connection was just made but the soon to arrive request data simply  
11 has not arrived yet. In this case, a legitimate connection request would be denied.

12 However, this case would typically be relatively rare. For example, the legitimate  
13 connection request would not be denied unless the backlog queue had entries in it which  
14 should in itself be relatively rare. Secondly, even though the backlog queue is full, the  
15 period of time between the time a connection is made and the time the data is received is  
16 relatively brief for a legitimate connection request. Thus, the chance that the legitimate  
17 connection request would be executing in that brief period is also relatively small. On the  
18 other hand, using this method would substantially reduce the impact of denial of service  
19 attacks. Thus, the advantages of the method in reducing the impact of denial of service  
20 attacks would typically outweigh the relatively small risk of denying legitimate connection  
21 requests.

22 Notwithstanding this small risk, the method may be further optimized to reduce the  
23 chances for denying legitimate connection requests even further. For example, the server  
24 computer system 220 may be configured to allow for a specified grace period after entries

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

10 What is claimed and desired to be secured by United States Letters Patent is: